Privacy Itch and Scratch: On Body Privacy Warnings and Controls

Conference or Workshop Item

Privacy Itch and Scratch: On Body Privacy Warnings and Controls

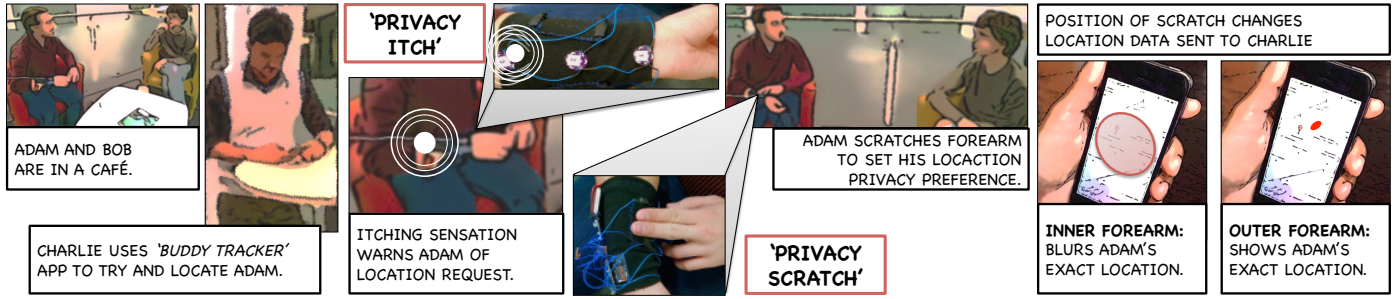

Figure 1: Use case scenario for on body privacy warnings and controls

Vikram Mehta
The Open University, UK
vikram.mehta@open.ac.uk

Blaine A. Price
The Open University, UK
b.a.price@open.ac.uk

Arosha K. Bandara
The Open University, UK
arosha.bandara@open.ac.uk

Bashar Nuseibeh
The Open University, UK
Lero, Ireland
bashar.nuseibeh@open.ac.uk

CHI'16 Extended Abstracts, May 07-12, 2016, San Jose, CA, USA
ACM 978-1-4503-4082-3/16/05.
http://dx.doi.org/10.1145/2851581.2892475.

Abstract

In the age of ubiquitous computing increasing amounts of personal data are being logged and shared, making privacy management a challenging task that must be integrated into our daily lives. In this paper, we explore the metaphors of 'privacy itch' for warnings and 'privacy scratch' for control of privacy preferences through real time, on-body, haptic interaction technologies. To assess the utility of these concepts, we implemented a forearm wearable prototype: the Privacy Band, and conducted a small lab-based user study.

Author Keywords

User privacy management; Haptic warnings; Wearable computing; On-body interfaces.

ACM Classification Keywords

H.5.2. Information interfaces and presentation: Haptic I/O; K.4.1 Computers and Society: Privacy

Introduction

With the rapid growth in pervasive/ubiquitous computing, personal information privacy has become a bottleneck research challenge [9,13,21]. A lot of private and often sensitive information about users that is collected through ubiquitous devices can be shared with unknown entities at any time, without them being aware. In order to control which of their personal data is being collected, who can collect such data, and when this is allowed, users currently need to go through and pre-set privacy rules for devices/applications they want to use [2,11,12]. Even then, controlling the diffusion of such information has become an increasingly daunting task, especially due to the innumerable possibilities of information flow and varying privacy preferences of users across different contexts. Moreover, setting privacy rules is a complex and time-consuming process which many people are unwilling [5] to do until their privacy is violated, thus increasing the risk of personal information privacy breaches. When such breaches (highly privacy sensitive or ambiguous, in particular) occur, appropriate interfaces are required to sensitively and actively warn users in real time, enable them to take immediate action when informed, and learn from their responses. Therefore these interfaces need to be direct, intuitive, inherently private and predominantly non-obtrusive to the user. To fulfil such requirements, we propose providing users with real time, on body, haptic, personal information privacy warnings as a metaphorical 'privacy itch' at distinct locations on the volar (inner) surface of their forearm. We extend the metaphor to include users' responses to these warnings as a 'privacy scratch' on the sides of their forearm. Thus a potential privacy breach will cause an itch, which the user can scratch in response, enabling her to actively control the release of sensitive information in a suitable, innocuous, continuous and eyes free manner. In the following sections we discuss the related work and key characteristics of such on-body privacy awareness and control systems. This is followed by a description of the design of our wearable prototypical implementation: the Privacy Band, with non-obtrusive but reactive interaction capabilities, along with a user study. The paper concludes with a discussion of the results and some thoughts on future work.

On-body privacy warnings and controls

In order to examine where on-body privacy warnings might be used, consider the following use case scenario presented in Figure 1. Adam has a wide network of friends and enables the Buddy Tracker app on his smartphone, which allows selected friends to locate him for serendipitous meetings. He wants to have some control over his privacy so he connects the Buddy Tracker app to the Privacy Band. While sitting in a café with Bob he feels a slight itch on his forearm indicating that someone has checked his location. He does not want his chat with Bob to be disturbed so he subtly scratches the inner side of his forearm indicating that he wants to keep this information private and the Buddy Tracker app stops revealing his location. If instead he wanted to meet someone at the café he could have scratched his outer forearm to indicate that he is happy for his location to be shared by the app.

Motivation and Related Work

Feedback about privacy-affecting system operations is important for informed end-user privacy management [19]. Most authors use off-body notification techniques (on mobile phones) to notify end users of any privacy breach, but this is not as immediate, nor as available as on-body input/output systems [7,8,17]. Interacting

with ones' own body is very personal and private in nature. The proprioception and exteroception effect of the human body also helps in eyes-free input and output, eliminating the need for visual attention. Such interfaces are easy to reach and interact on, and offer users with possibilities of continuous, non-obtrusive and inherently private interactions. The forearm in particular is the most user preferred, on-body interaction location [6,23]. It has a naturally hybrid nature and can be used as a surface for public (outer forearm) and private (inner forearm) interactions [18,23]. Users can interact precisely with their forearms by dividing their forearm space into 6 or 7 distinctive points, in an eyes-free manner [7,15]. This inspired us to use appropriate input-output points on the user's forearm for privacy feedback and control.

Haptic feedback in particular has been proposed as a basis for private, non-verbal communication by several authors [3,4,16,20] who investigated the communication capacity of haptic/tactile feedback for complex messages in a completely non-visual, non-auditory setting. Warning users through haptic stimulation can be distinctive and unanticipated [15,16], helping users to re-focus their attention. The silent, non-visual and individually communicated, nature of haptic feedback makes it ideal for communicating private information. Also, it makes authentication of an action more intuitive. Privacy-Shake [8] particularly, focused on how haptic interfaces and interactions could help manage personal information privacy. However, users' feedback on the interactions involved (shaking of the mobile phone) indicated that Privacy-Shake was awkward and obtrusive to use.

A number of researchers have previously investigated haptic systems [7,14,16]. In [7], the authors discuss vibrotactile localization on the volar forearm along 7 linear points between the wrist and the elbow. This demonstrates that the forearm can be divided into multiple, user recognizable stimulus sites. Moreover, in [14,16], the authors talk about Tactograms (or tactile patterns) and the associated control parameter variations that can enrich haptic warnings.

Key Characteristics

Our review of the relevant literature highlights key characteristics of privacy warnings and haptic interfaces that inform our choice of essential features of an on-body haptic privacy warning system. We elaborate these features below and explain our rationale for including them in our prototype Privacy Band, described later in the paper.

DISTINCT WARNING LOCATIONS

In order to communicate a range of warnings, the system must have different personal data categories mapped to distinct points on the body interface. This allows us to explore how users tolerate different sensitivities of privacy breach data haptically.

DIFFERENT WARNING MODES

Variation in control parameters (e.g., intensity, frequency, duration, modulation, sequences) can help to communicate different predefined meanings and express variability of privacy breaches. For instance, a high intensity and repetitive vibration can be inferred as a critical privacy warning (e.g., someone trying to access users' credit card information or users' location more than 'X' times in a short duration, where 'X' can be any pre-set integer threshold). A low intensity and

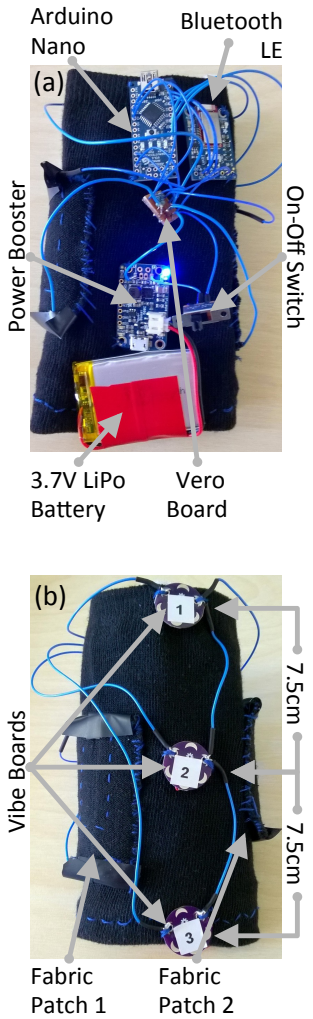

Figure 2: Privacy Band
(a)"Front" View (b)"Back" View

repetitive vibration might indicate less critical breach or a mild warning (e.g. someone trying to access users' location less than 'X' times).

REACTIVE INPUT
In addition to notifying the user (output) the interface needs to be able to take input from the user to acknowledge and stop the feedback and indicate the user's wishes with respect to the warning: ignore it or take defensive action.

COMPLEMENTS OTHER OUTPUT DEVICES
As this is a haptic interface, it can complement both output and input from other devices including smart watches and smartphones.

Privacy Band

The Privacy Band is an on-body user interface for privacy warnings and their control. Previous research describes various models or tools such as Dynamic Bayesian Networks [1] or PROTOSS [10] that can detect an on going, or predict a future personal information privacy breach. Similarly, Yang et al. [24] provide a model to calculate the potential privacy risk of users' online information. We suggest that the Privacy Band could be integrated with such systems to provide warnings of possible privacy invasions.

Design and Implementation
Our prototype is a thin interactive e-band worn on the forearm. We used a thin, flexible and elastic fabric band (cut from flight socks) of dimensions [15 cm x 8 cm]. The front side (see Figure 2(a)) has an Arduino Nano v3.0 micro-controller, a low energy Bluetooth module, a PowerBoost 500C chip, an On-Off switch and a 3.7V LiPoly battery. The reverse (see Figure 2(b)) consists of 3 vibe boards (vibration amplitude 0.8G) placed at 7.5 cm intervals. This effectively divides the user's forearm into 3 distinct points when the Privacy Band is worn. The vibe boards are connected to the analog outputs of the Arduino to create variations in vibration intensity: High at 255, Low at 125. High vibration intensity refers to a critical warning, and low refers to a mild warning. The outer (away from the user) and inner (towards the user) sides are each sewn with a pressure sensitive fabric button (sandwiched Velostat between two pieces of fabric fused with conductive fabric, so that the conductive fabric faces inwards, towards each other, separated only by the Velostat), indicated as Fabric Patch 1 & 2 in Figure 2. All components are connected together through a small Veroboard in the center.

Our Android application to simulate privacy breaches connects to the Privacy Band via Bluetooth. Depending upon the generated (category and the variation) data privacy breach, the app instructs the band when and how to vibrate. The corresponding vibe boards then vibrate accordingly (until the user responds) and the user is haptically warned on his forearm. Users are briefed about the vibe board categorization on their forearm, so they could understand in which data category the privacy breach is "on going" or has "just occurred", in an eyes free manner.

To respond to the warnings, the user can simply scratch on the sides of the band without any need to look at it. A scratch on the outer side enables the user to ignore the privacy warning, and one on the inner side enables him to block the access of unintended recipient to the corresponding data item. Note that we use the word "scratch" to denote any sort of touch input to an area of the band such as scratching,

pressing, sliding with pressure, squeezing, shearing or twisting by the user.

User Study

After obtaining institutional ethics approval, we recruited 11 participants (4 female; mean age 31.64y; median 29y) from among staff and students at our university. Each session was video recorded and lasted for around 30 minutes. Throughout the study, users were asked to wear the Privacy Band on their non-dominant forearm with vibe board 1 closer to the wrist and vibe board 3 towards the elbow. The study started with a 2-minute training task, which helped participants to understand the feel of each vibrating point at high and low, intensities on their forearm. For our evaluation we virtually mapped each vibeboard to 3 categories of personal data (1) Financial information (e.g., banking credentials, credit card info.); (2) Photo sharing on social networks; and (3) Location disclosure. These categories are chosen as common representative items from the 14 personal information items found to be a privacy risk on mobile devices in the user study conducted by Jorgensen et al. [9].

In the main task (with 165 trials), we explored how users reacted to and interacted with the Privacy Band while doing a randomized series of 3 real world tasks involving visual, auditory and physical distractions ((a) set up a new payee in bank account, (b) watching videos and guessing movie names, and (c) playing the drawing game Pictionary). At the beginning, users were told the data category assigned to each vibe board. During the study we generated random data, i.e. not data belonging to users, to simulate privacy warnings (in a 'Wizard of Oz' style) and sent these to the user haptically through the Privacy Band.

Results and Discussion

The aim of this user study was not to evaluate the technology of Privacy Band, but to evaluate the utility of the concept of on-body privacy management. The overall user response to which, was quite positive. With many remarking that it was convenient, *"useful"* for *"immediate/urgent response"* (P3, P6, P7, P8, P10) and effective as *"you could talk, feel and react at the same time"* (P9). Further confirmation of this convenience included: *"I will prefer this. It is very convenient as I just have to click a button and don't have to get tensed about what is happening with my data"* (P3). Most importantly, it gave users a sense of control over their data: *"If given a choice, I would of course use this type of device because then I can have a better say, as opposed to someone else dictating what has to be done with my data"* (P5).

82% of the privacy itch warnings resulted in the user choosing to block the information flow, irrespective of their type or intensity. This was due to several underlying factors:

LACK OF INFORMATION. An itch could convey only one dimension of information to the user, i.e. the severity of the breach. This explains us that itch with difference in severity only may not be the most ideal method of privacy breach notification on its own and could be made richer by including other control parameters (see page 3) to convey more information.

HIGH CONCERN FOR DATA PRIVACY. 3 participants (P4, P8, P10) blocked all the breaches because they didn't want any of their information to be accessed.

PERSONAL PREFERENCES. Some participants established certain rules of what to block or ignore. Financial breach was always blocked when at high intensity, and 83% of times when at low intensity. *"I said I was going to allow only low vibration for pictures and I didn't feel that"*, made P9 block every breach he encountered. *"I don't care much about my pictures or where I am, so I just ignored some of those breaches"*, said P11.

LACK OF CERTAINTY. When a participant was unsure of the category or intensity of vibration, he chose to block the data flow. *"Anyways I am blocking it so I am safe so why should I think about the categories"*, said P3.

Limitations and Future Work

Our prototype realises a simplified solution for end users' privacy management needs, and does not consider factors such as the users' context, recipient identity, etc., which will influence the privacy choices. This is because our main intention with this work is to take a step towards exploring the concept of on-body warnings and privacy management, not to build and evaluate a sophisticated on-body privacy management device. For a more realistic exploration however, future prototypes must investigate ways of incorporating richer contextual information to support privacy control decisions, which was a need also identified by our study participants: *"I would be really irritated if every single time my data is accessed and input is sent"* (P5), *"When I am working in the department, it might get too annoying for me"* (P3), and *"Who is accessing my data, is it my wife? (P10)"*.

Participants reported difficulty in detecting the category and intensity of breaches while doing various sub tasks, especially while playing Pictionary. This exposes obvious limitations of non-obtrusive haptics during physical activities. However, various other factors such as user's forearm geometry, different positional arrangement of the vibe boards and variations in tactile control parameters other than intensity, must also be taken into consideration. In addition to needing improvements to match the fit of the band to the user's forearm, our prototype would also benefit from having a more attractive visual appearance. Skin worn sensors such as iSkin [22] could be used to create aesthetic and more fitting designs of Privacy Band in the future.

Conclusions

Managing user privacy is a highly complex task and this work looks at it through a different lens. We have proposed the concept of using on-body haptic interfaces for appropriately alerting users about personal data privacy breaches, and providing them the ability to control their data in a direct but non-obtrusive manner. We have presented a forearm wearable prototypical implementation, the Privacy Band, with non-obtrusive but reactive interaction capabilities. Our user study confirms the usefulness and effectiveness of the privacy itch and privacy scratch interaction metaphors for managing data privacy and opens up a promising stream of further research in this area.

Acknowledgments

We acknowledge ERC Advanced Grant 291652 (ASAP) and EPSRC Grant EP/K033522/1 (Privacy Dynamics).

References

1. An, X., Jutla, D., and Cercone, N. Privacy intrusion detection using dynamic Bayesian networks. *ACM Int. Conf. Proc. Series*, (2006), 208–215.

2. Choe, E.K., Jung, J., Lee, B., and Fisher, K. Nudging people away from privacy-invasive mobile apps through visual framing. In *Human-computer interaction–INTERACT*. Springer, 2013, 74–91.
3. Cholewiak, R.W. and Collins, A.A. Vibrotactile localization on the arm: Effects of place, space, and age. *Perception & psychophysics 65*, 7 (2003), 1058–1077.
4. Van Erp, J.B., Van Veen, H.A., Jansen, C., and Dobbins, T. Waypoint navigation with a vibrotactile waist belt. *ACM Transactions on Applied Perception 2*, 2 (2005), 106–117.
5. Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., and Wagner, D. Android permissions: User attention, comprehension, and behavior. *Proc. of the 8th Symposium on Usable Privacy and Security*, ACM (2012), 3.
6. Harrison, C. and Faste, H. Implications of location and touch for on-body projected interfaces. *Proc. of the 2014 Conf. on Designing interactive systems*, ACM (2014), 543–552.
7. Harrison, C., Ramamurthy, S., and Hudson, S.E. On-body interaction: armed and dangerous. *Proc. of the 6th Int. Conf. on Tangible, Embedded and Embodied Interaction*, ACM (2012), 69–76.
8. Jedrzejczyk, L., Price, B.A., Bandara, A.K., and Nuseibeh, B. Privacy-shake: a haptic interface for managing privacy settings in mobile location sharing applications. *Proc. of the 12th Int. Conf. on Human computer interaction with mobile devices and services*, ACM (2010), 411–412.
9. Jorgensen, Z., Chen, J., Gates, C.S., Li, N., Proctor, R.W., and Yu, T. Dimensions of risk in mobile applications: A user study. *Proc. of the 5th Conf. on Data and Application Security and Privacy*, ACM (2015), 49–60.
10. Kafali, O., Gunay, A., and Yolum, P. PROTOSS: A Run Time Tool for Detecting Privacy Violations in Online Social Networks. *Int. Conf. on Advances in social networks analysis and mining*, IEEE (2012), 429–433.
11. Kelley, P.G., Bresee, J., Cranor, L.F., and Reeder, R.W. A nutrition label for privacy. *Proc. of the 5th Symposium on Usable Privacy and Security*, ACM (2009), 4.
12. Kelley, P.G., Cranor, L.F., and Sadeh, N. Privacy as part of the app decision-making process. *Proc. of the Conf. on Human Factors in Computing Systems*, ACM (2013), 3393–3402.
13. Langheinrich, M. Privacy invasions in ubiquitous computing. *Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing*, ACM (2002).
14. Lee, S.C. and Starner, T. BuzzWear: alert perception in wearable tactile displays on the wrist. *Proc. of the Conf. on Human Factors in Computing Systems*, ACM (2010), 433–442.
15. Lin, S.-Y., Su, C.-H., Cheng, K.-Y., Liang, R.-H., Kuo, T.-H., and Chen, B.-Y. Pub-point upon body: exploring eyes-free interaction and methods on an arm. *Proc. of the 24th Symposium on User interface software and technology*, ACM (2011), 481–488.
16. Matscheko, M., Ferscha, A., Riener, A., and Lehner, M. Tactor placement in wrist worn wearables. *Int. Symposium on Wearable Computers*, IEEE (2010), 1–8.
17. Mistry, P., Maes, P., and Chang, L. WUW-wear Ur world: a wearable gestural interface. *Extended abstracts on Human factors in computing systems*, ACM (2009), 4111–4116.
18. Olberding, S., Yeo, K.P., Nanayakkara, S., and Steimle, J. AugmentedForearm: exploring the design space of a display-enhanced forearm. *Proc. of the 4th Int. Conf. on Augmented Human*, ACM (2013), 9–12.
19. Patil, S., Hoyle, R., Schlegel, R., Kapadia, A., and Lee, A.J. Interrupt now or inform later?: Comparing

immediate and delayed privacy feedback. *Proc. of the 33rd Conf. on Human Factors in Computing Systems*, ACM (2015), 1415–1418.

20. Sherrick, C. Vibrotactile Pattern Perception: Some Findings and Applications. In *The psychology of touch*. 2013, 189.

21. Stankovic, J.A. Research Directions for the Internet of Things. *IEEE Internet of Things Journal*, 1 (2014), 3–9.

22. Weigel, M., Lu, T., Bailly, G., Oulasvirta, A., Majidi, C., and Steimle, J. iSkin: flexible, stretchable and visually customizable on-body touch sensors for mobile computing. *Proc. of the 33rd Conf. on Human Factors in Computing Systems*, ACM (2015), 2991–3000.

23. Weigel, M., Mehta, V., and Steimle, J. More than touch: understanding how people use skin as an input surface for mobile computing. *Proc. of the 32nd Conf. on Human Factors in Computing Systems*, ACM (2014), 179–188.

24. Yang, M., Yu, Y., Bandara, A.K., and Nuseibeh, B. Adaptive sharing for online social networks: a trade-off between privacy risk and social benefit. *Proc. of the 13th Int. Conf. on Trust, Security and Privacy in Computing and Communications*, IEEE (2014), 45–52.